

Ukryte kamery w miejscu pracy

W naszym poprzednim artykule analizowaliśmy wyrok Trybunału Sprawiedliwości Unii Europejskiej dotyczący konieczności i warunków wyrażania zgody na pliki cookies. Dzisiejsza publikacja dotyczyć będzie orzeczenia innego europejskiego organu wymiaru sprawiedliwości tj. Europejskiego Trybunału Praw Człowieka w Strasburgu.

17 października 2019 r. Wielka Izba ETPC w składzie 17 sędziów (głosami 14 sędziów przy 3 zdaniach odrębnych) wydała wyrok w sprawie *López Ribalda i inni przeciwko Hiszpanii*. W wyroku tym uznano, że **stosowanie wobec pracowników ukrytego nadzoru za pomocą kamer może być usprawiedliwione w określonych sytuacjach**.

Stan faktyczny

Sprawa, która trafiła do ETPC, dotyczyła ukrytego monitoringu pracowników w hiszpańskiej sieci supermarketów.

Z uwagi na stwierdzone nieprawidłowości, w tym m.in. różnicę między stanem magazynu a wartością dziennej sprzedaży, kierownik sklepu zdecydował się na zainstalowanie w placówce **dwóch rodzajów kamer: widocznych oraz ukrytych**.

Widoczne kamery miały służyć przeciwdziałaniu kradzieżom przez klientów. O ich instalacji zostały poinformowani wszyscy kasjerzy. Kamery ukryte miały monitorować z kolei zachowanie pracowników. O nich nie został poinformowany żaden z pracowników.

Po 10 dniowym nadzorze, ukryte kamery zarejestrowały, że czternaście kasjerek pomagało w kradzieży, jak i samodzielnie kradło towar. Wszystkie te kasjerki zostały zwolnione dyscyplinarnie.

Część z nich odwołała się do hiszpańskiego sądu pracy wskazując, że zwolnienie nie było dopuszczalne, bo pracodawca wykorzystał nagrania z ukrytego monitoringu, który z kolei naruszył ich prywatność. Nagrania te nie powinny tym samym stanowić dowodu. W obu instancjach sędziowie przyznali jednak rację pracodawcy i sprawa trafiła do ETPC.

Byłe pracownice twierdziły, że złamane zostały art. 8 i 6 *Europejskiej Konwencji Praw Człowieka* (prawo do prywatności i sprawiedliwego procesu). Izba Trybunału uznała, że doszło do naruszenia art. 8, ale nie art. 6 *Konwencji*. Po odwołaniu sprawa trafiła do Wielkiej Izby, a ta zmieniła wyrok wskakując, że **do naruszenia w ogóle nie doszło**.

Sędziowie wskazali, że w przedmiotowej sprawie **należy przede wszystkim wyważyć prawo pracownika do ochrony prywatności oraz interes pracodawcy**, który może chronić swój majątek i dbać o prawidłowe prowadzenie działalności.

Odnosząc się do zgodności działania pracodawcy z art. 8 *Europejskiej Konwencji Praw Człowieka* Trybunał uznał, że należy w tym celu wziąć pod uwagę szereg elementów, takich jak:

- kwestię poinformowania pracownika o możliwym stosowaniu takich form nadzoru pracy,





- zakres monitoringu,
- stopień ingerencji monitoringu w prywatność pracownika oraz jej możliwe konsekwencje,
- prawnie uzasadnione powody wprowadzenia takiego nadzoru,
- możliwość zastosowania innych, mniej inwazyjnych środków, którymi można osiągnąć ten sam cel,
- stosowane środki ochronne.

Odnosząc powyższe kwestie do stanu faktycznego sprawy, sędziowie wskazali, że **ingerencja w prywatność pracowników nie osiągnęła wysokiego poziomu istotności**, m.in. z uwagi na:

- istnienie uzasadnionego podejrzenia, że dokonano poważnego wykroczenia oraz zakres ujawnionych strat, które mogą stanowić ważne uzasadnienie braku poinformowania pracowników o monitoringu,
- monitorowana przestrzeń miała charakter otwartej przestrzeni sklepowej, nie stanowiła zatem miejsca, wobec którego oczekuje się wysokiego stopnia prywatności jak np. łazienka czy szatnia,
- nadzór trwał tylko 10 dni, podczas których dokonano identyfikacji odpowiedzialnych pracowników,
- dostęp do nagrań miał ograniczony krąg odbiorców,
- nagrań nie wykorzystano do innych celów niż potwierdzenie kradzieży,
- pracodawca nie miał innego sposobu na udowodnienie naruszeń.

Biorąc powyższe pod uwagę, ETPC wskazał, że w omawianym przypadku nie doszło do naruszenia art. 8 *Konwencji*.



Monitoring zgodny z RODO – praktyczny pakiet procedur, wytycznych i klauzul

Stosujesz monitoring (wizyjny lub aktywności pracowników)? Jesteś zobowiązany do wdrożenia odpowiedniej dokumentacji regulującej te kwestie.

Aby ułatwić Ci zadanie przygotowaliśmy dla Ciebie kompleksowy pakiet wytycznych i procedur związanych z monitoringiem.

SPRAWDŹ





Co z wyrokiem w sprawie Copland?

Październikowy wyrok odbiega od linii orzeczniczej przyjętej wcześniej przez Trybunał w sprawach związanych z monitoringiem pracowników. Linie tę w 2007 r. wyznaczył wyrok w sprawie *Copland przeciwko Zjednoczonemu Królestwu*. Od tego wyroku w swoich orzeczeniach ETPC uznawał, że **pracodawcy nie mogą stosować ukrytego monitoringu pracowników**.

Lynette Copland była asystentką w szkole państwowej Carmathenshire College. Podczas trwania zatrudnienia, jej telefon, poczta elektroniczna oraz połączenia internetowe były monitorowane przez przełożonego. Rząd brytyjski twierdził, że celem prowadzonego monitoringu było ustalenie czy pracownik nie nadużywa urządzeń szkoły dla celów prywatnych. Według rządu monitoring telefonu polegał na analizie rachunków telefonicznych pod kątem numerów, z którymi łączyła się Pani Copland, dat i czasu połączeń oraz ich długości i kosztów. Monitoring korespondencji elektronicznej miał polegać na analizie adresów e-mailowych odbiorców oraz daty i czasu ich wysyłania, a monitorowanie użytkownika Internetu, miało przybrać postać analizy odwiedzanych stron, daty i czasu odwiedzin oraz długości ich trwania.

Zdaniem skarżącej, monitoring jej aktywności poszedł o wiele dalej i w jego zakresie zastosowano również dokładną i całościową analizę połączeń telefonicznych (czasu, liczby połączeń oraz numerów telefonicznych). Pani Copland utrzymywała również, że pracodawca oddzwaniał na analizowane numery w celu sprawdzenia ich użytkowników.

W związku z powyższym, skarżąca zarzuciła Zjednoczonemu Królestwu naruszenie przede wszystkim art. 8 *Europejskiej Konwencji Praw Człowieka* wskazującej m.in. na prawo każdego do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

W swoim rozstrzygnięciu ETPC wskazał, że **rozmowy telefoniczne z pracy, e-maile oraz korzystanie z Internetu są objęte terminami „życie prywatne” i „korespondencja”**.

Trybunał podkreślił też, że skarżąca **nie została nigdy poinformowana o możliwym monitorowaniu** jej działań, a zatem miała ona uzasadnione oczekiwanie zachowania ich prywatności. ETPC orzekł, że gromadzenie i przechowywanie zgromadzonych podczas prowadzenia monitoringu danych, stanowi naruszenie art. 8 *Europejskiej Konwencji Praw Człowieka*.

Pani Copland przyznano wówczas 3 tys. funtów zadośćuczynienia za szkody niemajątkowe oraz 6 tys. funtów tytułem poniesienia kosztów i wydatków związanych ze skargą.

Podobna argumentacja i stanowisko ETPC pojawiało się przy innych orzeczeniach, m.in.:

- *Barbulescu przeciwko Rumunii* z 2017 r. – dotyczącym kontroli prywatnej korespondencji pracownika wysyłanej za pośrednictwem służbowego komunikatora, gdzie kluczowym dla Trybunału był **brak poinformowania pracownika o prowadzonej kontroli**,
- *Antovic i Mirkovic przeciwko Czarnogórze* z 2017 r. – dotyczącym legalności monitoringu wizyjnego zainstalowanego w salach wykładowych, gdzie ETPC konsekwentnie wskazał, że monitoring był bezprawny oraz zaznaczył, że **prawo do prywatności dotyczy również działalności zawodowej pracownika**.





Biorąc pod uwagę wskazane wyżej orzeczenia i zestawiając je z wyrokiem w sprawie *López Ribalda i inni przeciwko Hiszpanii*, należy stwierdzić, że ETPC zmienił swoje stanowisko i argumentację w zakresie ram kontroli pracownika przez pracodawcę.

Stanowisko Prezesa UODO

Do wyroku ETPC polski organ nadzoru odniósł się m.in. w 8 wydaniu *Newslettera UODO dla inspektorów ochrony danych*. Podkreślił, że w polskim systemie prawnym zasady stosowania monitoringu w miejscu pracy uregulowane są w art. 22² Kodeksu pracy.

Zgodnie z powoływanym przepisem **monitoring może służyć wyłącznie enumeratywnie wyliczonym celom**, tj.:

- zapewnieniu bezpieczeństwa pracowników lub ochrony mienia, lub
- kontroli produkcji, lub
- zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Regulacje te jasno określają, że **pracodawca oznacza pomieszczenia i teren monitorowany** w sposób widoczny i czytelny. Oznaczenie powinno nastąpić nie później niż jeden dzień przed uruchomieniem monitoringu.

Prezes UODO przypomina również, że **konieczna w tym zakresie jest realizacja tzw. obowiązku informacyjnego** z art. 13 RODO, zgodnie z którym w momencie gromadzenia danych, administrator powinien poinformować osobę, której dane dotyczą m.in. o swojej tożsamości, celach i podstawach prawnych przetwarzania, a także o przysługujących jej w związku z tym przetwarzaniem prawach.

O tym jak prawidłowo realizować obowiązki informacyjne wobec podmiotów danych pisaliśmy na naszym blogu [tutaj](#).

W swoim stanowisku, polski organ nadzoru poucza również, że w przypadku, gdy osoby objęte monitoringiem są przekonane, że doszło do naruszenia ich danych osobowych, mogą złożyć **skargę na administratora do Prezesa UODO**. Niezależnie od tego, czy się na to zdecydują mogą również **dochodzić swoich praw przed sądem cywilnym** co przewiduje art. 79 RODO.

Dodatkowo, każda osoba, która uważa, że w wyniku naruszenia przepisów RODO poniosła szkodę majątkową lub niemajątkową, **ma też prawo żądać odszkodowania**, do czego uprawnia ją art. 82 RODO.

W kolejnym swoim stanowisku przygotowanym w odpowiedzi na zapytanie Dziennika Gazety Prawnej, UODO wskazał, że wyrok ETPC **nie ma charakteru ogólnego**. Odnosi się do konkretnych przepisów przyjętych przez ustawodawcę hiszpańskiego, których to zgodność z *Konwencją* była oceniana.

Wyrok w sposób bezpośredni i jednoznaczny wskazuje w paragrafie 118, że to **ustawodawca krajowy decyduje o sposobie, w jaki godzi się interesy stron**, takie jak prawo do ochrony prywatności jednostki oraz prawo do ochrony mienia przez pracodawcę. I o ile ustawodawca





hiszpański uregulował te kwestie w sposób ogólny, to już jego polski odpowiednik zrobił to w sposób bardziej szczegółowy, określając w powoływanych przepisach *Kodeksu pracy* m.in. formy monitoringu.

ETPC a RODO i sprawa polska

Po opublikowaniu wyroku ETPC, wiele ekspertów komentowało go wskazując krótko: *wygrał zdrowy rozsądek*. Trudno się z tym nie zgodzić. Hiszpański pracodawca ponosił regularne straty finansowe związane z działaniem swoich pracowników. I co kluczowe dla całej sprawy, **nie miał w tym zakresie innych możliwości by skutecznie przeciwdziałać nadużyciom**, których dopuszczali się jego pracownicy.

Jest to pierwszy wyrok, który tak jednoznacznie przesądza możliwość stosowania ukrytego monitoringu jako formy kontroli działań pracownika. Wyrok ten daje również jasne wskazówki, kiedy taka kontrola jest dopuszczalna, tj. kiedy interes pracodawcy będzie przeważał nad interesem i prawem do prywatności pracownika.

Zdrowy rozsądek, który objawił się w Wielkiej Izbie ETPC nie oznacza jednak, że polscy pracodawcy mogą od razu zacząć instalować u siebie ukryte kamery. Polskie przepisy *Kodeksu pracy* określając warunki monitoringu, wskazują bowiem jasno, że taki rodzaj monitoringu nie jest dopuszczalny. Stanowisko Prezesa UODO w tym zakresie też nie pozostawia wątpliwości.

Aby ukryty monitoring stosowany mógł być przez polskiego pracodawcę, **zmianie ulec muszą przepisy *Kodeksu pracy***. W innym przypadku, polskie sądy z całym prawdopodobieństwem orzekać będą na niekorzyść zatrudniającego. Pytanie, który z nich doprowadzi w przyszłości Polskę przed Trybunał.

W omawianym przypadku, pozostają jeszcze **dwie kwestie związane z respektowaniem przepisów RODO**, tj.:

- **podstawa prawna** przetwarzania danych z ukrytego monitoringu – w tym zakresie podstawę stanowiłby art. 6 ust. 1 lit f) RODO tj. prawnie uzasadniony interes pracodawcy jako administratora danych. Oczywiście interes ten powinien zostać odpowiednio wyważony, a przed wdrożeniem takiego rozwiązania, administrator powinien przeprowadzić tzw. *balancing test*, określając czy rzeczywiście w konkretnym przypadku interes pracodawcy stoi wyżej niż interes pracownika (osoby, której dane dotyczą).
- sposób dopełnienia **obowiązku informacyjnego**, o którym mowa w art. 13 RODO – wyrok ETPC nie rozstrzyga kwestii związanej z obowiązkiem poinformowania osób, których dane są przetwarzane przez administratora. Taki obowiązek istnieje praktycznie zawsze, gdy administrator gromadzi dane bezpośrednio od osoby, której dane dotyczą. RODO w tym zakresie przewiduje możliwość zwolnienia tylko w przypadku, kiedy podmiot danych posiada już takie informacje. Jako, że informacje podawane w klauzulach informacyjnych powinny być przejrzyste nie powinno się stosować sformułowań, które pozostawiałyby miejsce dla różnych ich interpretacji. W szczególności, należy unikać zwrotów, takich jak *może* czy *możliwe*. Administrator powinien zatem poinformować, że dane z monitoringu przetwarza, a nie że może się tak zdarzyć, że dane będzie gromadził jak zamontuje ukryte kamery.



Podsumowanie

Wyrok Europejskiego Trybunału Praw Człowieka w sprawie *López Ribalda i inni przeciwko Hiszpanii* nie daje automatycznie prawa polskim pracodawcom do instalacji ukrytych kamer monitorujących działania ich pracowników. **Dopóki zmianie nie ulegną przepisy Kodeksu pracy regulujące kwestię form monitoringu aktywności postępowanie takie będzie niezgodne z prawem.**

Wyrok ETPC zwraca jednak uwagę na bardzo ważny aspekt w działalności pracodawcy i otwiera dyskusję w zakresie konieczności zmian w polskich przepisach. Są bowiem takie sytuacje, kiedy wyłącznie forma ukrytej kontroli może przynieść pracodawcy wymierne efekty. Zmiana tych regulacji *Kodeksu pracy* nie byłaby jednak łatwa. Sprzeciw związków zawodowych czy organizacji pracowników jest bowiem więcej niż pewny.

Autor artykułu:

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Źródła:

- [Wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 października 2019 r. w sprawie López Ribalda i inni przeciwko Hiszpanii \(sygn. 1874/13\)](#)
- [Wyrok Europejskiego Trybunału Praw Człowieka z dnia 5 września 2017 r. w sprawie Barbulescu przeciwko Rumunii \(sygn. 61496/08\)](#)
- [Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 listopada 2017 w sprawie Antovic i Mirkovic przeciwko Czarnogórze \(sygn. 70838/13\)](#)
- [Newsletter UODO dla inspektorów ochrony danych, numer 8/2019, listopad 2019](#)
- [Glosa do orzeczenia Europejskiego Trybunału Praw Człowieka w sprawie Copland przeciwko Zjednoczonemu Królestwu, Arkadiusz Lach, Monitor Prawa Pracy, 7/2007](#)
- [Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3 lipca 2007 r. w sprawie Copland przeciwko Zjednoczonemu Królestwu \(sygn. 62617/00\)](#)
- [Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2](#)
- [Stanowisko Urzędu Ochrony Danych Osobowych z 22 października 2019 r. wydane na prośbę DGP](#)

